UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

D-2 NASSIF SAMI DAHER,

Defendant.
_____/

Honorable Nancy G. Edmunds

Case no. 18-cr-20559

GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION TO DEFENDANT'S MOTION TO DISCOVER EVIDENCE SECURED PURSUANT TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED BY 50 U.S.C. §§ 1801-1812

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES

OTHER AUTHORITIES

I. INTRODUCTION

The Government is filing this unclassified Memorandum in Opposition to the Defendant's Motion to Discover Evidence Secured Pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), as Amended by 50 U.S.C. §§ 1801-1812 (Doc. 28). The defendant seeks: (1) a determination by the government regarding the submission of an affidavit from the Attorney General attesting that disclosure of "the FISA application, FISA Order, and all cogent materials thereto" (*i.e.*, the FISA materials) would harm the national security; (2) a copy of any such affidavit; (3) an *in camera*, *ex parte* review of the FISA materials by this Court to determine whether the surveillance was lawfully authorized and appropriately conducted; and (4) disclosure of the FISA materials. (Doc. 28 at 22-23).[1]

The defendant's motion has triggered this Court's review of the FISA materials to determine whether the FISA information was lawfully acquired and whether the electronic surveillance was made in conformity with an order of authorization or approval. FISA specifies:

> [W]henever a motion is made pursuant to subsection (e) . . . to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain or suppress evidence or information obtained or derived from electronic surveillance under this Act, the United States district court . . . shall . . . if the Attorney General files an affidavit under oath that

[1] **[CLASSIFIED MATERIAL REDACTED]**

> disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.

50 U.S.C. § 1806(f). The government is filing herewith such an affidavit.[2] Consequently, the government respectfully submits that, for the reasons set forth herein, this Court must conduct an *in camera*, *ex parte* review of the documents relevant to the defendant's motion in accordance with the provisions of 50 U.S.C. § 1806(f).[3]

The government respectfully submits that, for the reasons set forth below, and as the Court's *in camera*, *ex parte* review will show: (1) the electronic surveillance at issue was lawfully authorized and lawfully conducted in compliance with FISA; (2) disclosure to the defendant of the FISA materials and the government's classified submissions is not authorized because the Court is able to make an accurate determination of the legality of the electronic surveillance without disclosing the FISA materials or portions thereof; (3) the FISA materials

---

[2] The Attorney General's affidavit ("Declaration and Claim of Privilege") is filed both publicly and as an exhibit in the Sealed Appendix to this classified filing. *See* Sealed Exhibit 1.

[3] **[CLASSIFIED MATERIAL REDACTED]**

should not be disclosed; (4) the FISA information should not be suppressed;[4] and (5) no hearing is required.

A. BACKGROUND

[CLASSIFIED MATERIAL REDACTED]

On August 14, 2018, a grand jury in the Eastern District of Michigan returned an indictment charging Daher with four counts of wire fraud, in violation of 18 U.S.C. §§ 1343, 2 (Doc. 1).[5]

On September 12, 2018, pursuant to 50 U.S.C. § 1806(c), the United States provided notice to Daher and this Court that it "intends to offer into evidence, or otherwise use or disclose . . . information obtained or derived from electronic surveillance conducted pursuant to [FISA]." (Doc. 21). On February 8, 2019, Daher filed his motion. (*See* Doc. 28).

[CLASSIFIED MATERIAL REDACTED][6]

---

[4] Although the defendant's motion does not explicitly seek suppression of the FISA information, the defendant alleges that the government violated FISA's minimization procedures and obtained a FISA order in violation of the Fourth Amendment. (*See* Doc. 28 at 10, 13). To the extent that the defendant's arguments can be construed as supporting a motion to suppress, the government respectfully requests that this Court also deny suppression of the FISA materials.

[5] The indictment also charged Kamel Mohammad Rammal (Rammal) with 14 counts of wire fraud. On December 6, 2018, Rammal pled guilty to one count of wire fraud. On April 18, 2019, he was sentenced to one year and one day in prison.

[6] As a result of the redactions, the pagination and footnote numbering of the classified memorandum and the unclassified memorandum are different.

B. OVERVIEW OF THE FISA AUTHORITIES

[CLASSIFIED MATERIAL REDACTED]

1. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. The FISC's Findings

[CLASSIFIED MATERIAL REDACTED]

II. THE FISA PROCESS

A. OVERVIEW OF FISA[7]

Enacted in 1978, and subsequently amended, FISA authorizes the Chief Justice of the United States to designate eleven United States District Judges to sit as judges of the FISC. 50 U.S.C. § 1803(a)(1). The FISC judges are empowered to consider *ex parte* applications submitted by the Executive Branch for electronic surveillance and physical search when a significant purpose of the application is to obtain foreign intelligence information, as defined in FISA. As originally enacted, FISA required that a high-ranking member of the Executive Branch of government certify that "the purpose" of the FISA application was to obtain foreign intelligence information. In 2001, FISA was amended as part of the Uniting and

[7] The provisions of FISA that address electronic surveillance are found at 50 U.S.C. §§ 1801-1812; those that address physical search are found at 50 U.S.C. §§ 1821-1829. These two sets of provisions are in many respects parallel and almost identical. Citations herein are generally to the two sets of provisions in parallel, with the first citation being to the relevant electronic surveillance provision, and the second citation being to the relevant physical search provision. This Memorandum references the statutory language in effect at the time relevant to this matter.

Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act").[8] One change to FISA accomplished by the USA PATRIOT Act is that a high-ranking official is now required to certify that the acquisition of foreign intelligence information is "a significant purpose" of the requested surveillance. 50 U.S.C. § 1804(a)(6)(B).

FISA provides that the Attorney General may authorize the emergency employment of electronic surveillance and physical search if the Attorney General makes certain determinations set forth in the statute. *See* 50 U.S.C. §§ 1805(e)(1), 1824(e)(1).[9] Emergency electronic surveillance or physical search must comport with FISA's minimization requirements, which are discussed below. 50 U.S.C. §§ 1805(e)(2), 1824(e)(2).

B. THE FISA APPLICATION

FISA provides a statutory procedure whereby the Executive Branch may obtain a judicial order authorizing the use of electronic surveillance and/or physical search within the United States where a significant purpose is the collection of foreign intelligence information.[10] 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B). Under FISA, foreign intelligence information is defined as:

---

[8] Pub. L. No. 107-56, 115 Stat. 272 (2001).

[9] **[CLASSIFIED MATERIAL REDACTED]**

[10] **[CLASSIFIED MATERIAL REDACTED]**

> (1) information that relates to, and if concerning a United States person[11] is necessary to, the ability of the United States to protect against–
>
> > (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> >
> > (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
> >
> > (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to–
>
> > (A) the national defense or the security of the United States; or
> > (B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e); *see also* 50 U.S.C. § 1821(1) (adopting the definitions from 50 U.S.C. § 1801). With the exception of emergency authorizations, FISA requires that a court order be obtained before any electronic surveillance or physical search may be conducted.

An application to conduct electronic surveillance pursuant to FISA must contain, among other things:

> (1) the identity of the federal officer making the application;
>
> (2) the identity, if known, or a description of the specific target of the electronic surveillance;

---

[11] **[CLASSIFIED MATERIAL REDACTED]**

> (3) a statement of the facts and circumstances supporting probable cause to believe that the target is a foreign power or an agent of a foreign power, and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
>
> (4) a statement of the proposed minimization procedures to be followed;
>
> (5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
>
> (6) a certification, discussed below, of a high-ranking official;
>
> (7) a summary of the manner or means by which the electronic surveillance will be effected and a statement whether physical entry is required to effect the electronic surveillance;
>
> (8) the facts concerning and the action taken on all previous FISA applications involving any of the persons, facilities, or places specified in the application; and
>
> (9) the proposed duration of the electronic surveillance.

50 U.S.C. § 1804(a)(1)-(9).

1. <u>The Certification</u>

An application to the FISC for a FISA order must include a certification from a high-ranking Executive Branch official with national security responsibilities that:

> (A) the certifying official deems the information sought to be foreign intelligence information;
>
> (B) a significant purpose of the surveillance is to obtain foreign intelligence information;

> (C) such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) designates the type of foreign intelligence information being sought according to the categories described in [50 U.S.C. §] 1801(e); and
>
> (E) includes a statement of the basis for the certification that –
>
> > (i) the information sought is the type of foreign intelligence information designated; and
> >
> > (ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a)(6); *see also* 50 U.S.C. § 1823(a)(6).

2. Minimization Procedures

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting United States persons obtained through FISA-authorized electronic surveillance or physical search, including persons who are not the targets of the FISA authorities. FISA requires that such minimization procedures be:

> reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. §§ 1801(h)(1); *see* 1821(4)(A).

In addition, minimization procedures also include "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. §§ 1801(h)(3), 1821(4)(c).

[CLASSIFIED MATERIAL REDACTED]

3. Attorney General's Approval

FISA further requires that the Attorney General approve applications for electronic surveillance, physical search, or both, before they are presented to the FISC.

C. THE FISC'S ORDERS

Once approved by the Attorney General, the application is submitted to the FISC and assigned to one of its judges. The FISC may approve the requested electronic surveillance, physical search, or both, only upon finding, among other things, that:

> (1) the application has been made by a "Federal officer" and has been approved by the Attorney General;
>
> (2) there is probable cause to believe that (A) the target of the electronic surveillance and/or physical search is a foreign power or an agent of a foreign power, and that (B) the facilities or places at which the electronic surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power, or that the premises or property to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power;

(3) the proposed minimization procedures meet the statutory requirements set forth in section 1801(h) (electronic surveillance) and section 1821(4) (physical search);

(4) the application contains all of the statements and certifications required by section 1804 (electronic surveillance) or section 1823 (physical search); and

(5) if the target is a United States person, the certifications are not clearly erroneous.

50 U.S.C. §§ 1805(a)(1)-(4), 1824(a)(1)-(4).

FISA defines "foreign power" to mean –

(1) a foreign government or any component, thereof, whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments; or

(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

50 U.S.C. § 1801(a)(1)-(7); *see also* 50 U.S.C. § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

"Agent of a foreign power" means –

(1) any person other than a United States person, who—

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4);

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

(C) engages in international terrorism or activities in preparation therefore [sic];

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power; or

(2) any person who –

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraphs (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraphs (A), (B), or (C).

50 U.S.C. § 1801(b)(1) and (2); *see also* 50 U.S.C. § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

The FISA application must establish probable cause to believe the target is acting as an agent of a foreign power at the time of the application. *See United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 310 (D. Conn. 2008) (finding that the FISA information was lawfully collected and finding specifically that "[e]ach application contained facts establishing probable cause to believe that, at the time the application was submitted to the FISC, the target of the FISA collection was an agent of a foreign power . . . ."), *aff'd*, 630 F.3d 102, 129 (2d Cir. 2010); *United*

States v. Squillacote, 221 F.3d 542, 554 (4th Cir. 2000) (concluding that the FISA applications established "probable cause to believe that . . . [the targets] were agents of a foreign power at the time the applications were granted"); *Global Relief Found. Inc. v. O'Neill*, 207 F. Supp. 2d 779, 790 (N.D. Ill. 2002) (concluding that "the FISA application established probable cause . . . at the time the search was conducted and the application was granted"), *aff'd* 315 F.3d 748 (7th Cir. 2002). However, FISA provides that "[i]n determining whether or not probable cause exists . . . a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. §§ 1805(b), 1824(b).

If the FISC has made all of the necessary findings and is satisfied that the FISA application meets the statutory provisions, the FISC issues an *ex parte* order authorizing the electronic surveillance, physical search, or both, requested in the application. 50 U.S.C. §§ 1805(a), 1824(a). The order must specify:

> (1) the identity, if known, or a description of the specific target of the collection;
>
> (2) the nature and location of each facility or place at which the electronic surveillance will be directed or of each of the premises or properties that will be searched;
>
> (3) the type of information sought to be acquired and the type of communications or activities that are to be subjected to the electronic surveillance, or the type of information, material, or

> property that is to be seized, altered, or reproduced through the physical search;
>
> (4) the manner and means by which electronic surveillance will be effected and whether physical entry will be necessary to effect that surveillance, or a statement of the manner in which the physical search will be conducted;
>
> (5) the period of time during which electronic surveillance is approved and/or the authorized scope of each physical search; and
>
> (6) the applicable minimization procedures.

50 U.S.C. §§ 1805(c)(1), (2)(A), 1824(c)(1), (2)(A).

Under FISA, electronic surveillance or physical search targeting a United States person may be approved for up to 90 days, and those targeting a non-United States person may be approved for up to 120 days. 50 U.S.C. §§ 1805(d)(1), 1824(d)(1). Extensions may be granted, but only if the United States submits another application that complies with FISA's requirements. An extension for electronic surveillance or physical search targeting a United States person may be approved for up to 90 days, and one targeting a non-United States person may be approved for up to one year. 50 U.S.C. §§ 1805(d)(2), 1824(d)(2).

III. DISTRICT COURT'S REVIEW OF FISC ORDERS

FISA authorizes the use in a criminal prosecution of information obtained or derived from any FISA-authorized electronic surveillance, provided that advance authorization is obtained from the Attorney General, 50 U.S.C. § 1806(b), and that

proper notice is subsequently given to the court and to each aggrieved person against whom the information is to be used.[12] 50 U.S.C. § 1806(c)-(d). Upon receiving notice, an aggrieved person against whom the information is to be used may move to suppress the FISA information on two grounds: (1) the information was unlawfully acquired; or (2) the electronic surveillance was not conducted in conformity with an order of authorization or approval. 50 U.S.C. § 1806(e). In addition, FISA contemplates that a defendant may file a motion or request under any other statute or rule of the United States to discover or obtain applications, orders, or other materials relating to electronic surveillance, *i.e.*, the FISA materials. 50 U.S.C. § 1806(f).

A. THE REVIEW IS TO BE CONDUCTED *IN CAMERA* AND *EX PARTE*

In assessing the legality of FISA-authorized electronic surveillance, the district court:

> shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.[13]

---

[12] **[CLASSIFIED MATERIAL REDACTED]**

[13] **[CLASSIFIED MATERIAL REDACTED]**

50 U.S.C. § 1806(f). On the filing of the Attorney General's affidavit or declaration, such as has been filed here, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. §1806(f). Thus, the propriety of the disclosure of any FISA application or order to a defendant may not even be considered unless and until the district court has first concluded that it is unable to make an accurate determination of the legality of the acquired collection after reviewing the government's submissions *in camera* and *ex parte*. *See United States v. Amawi*, 695 F. 3d 457, 474 (6th Cir. 2012) (noting district court's "*in camera* review of the FISA materials"); *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982). If the district court is able to make an accurate determination of the legality of the electronic surveillance based on its *in camera*, *ex parte* review, then the court *may not* order disclosure of any of the FISA materials to the defense, unless otherwise required by due process. *See Abu-Jihaad*, 630 F.3d at 129 (quoting 50 U.S.C. § 1806(g)); *United States v. El-Mezain*, 664 F.3d 467, 566 (5th Cir. 2011); *United States v. Mohammad*, 339 F. Supp. 3d 724, 737 (N.D. Ohio 2018).

1. *In Camera, Ex Parte* Review Is the Rule

Federal courts have repeatedly and consistently held that FISA anticipates an *ex parte, in camera* determination is to be the rule, with disclosure and an adversarial hearing being the exception, occurring only when necessary. *See United States v. Amawi*, 531 F. Supp. 2d 832, 837 (N.D. Ohio 2008) ("Where on the basis of what it receives from the government *in camera* and under seal, a district court concludes that it can determine whether a FISA surveillance and search was lawful, it may not order disclosure of any of the FISA materials."), *aff'd* 695 F.3d 457 (6th Cir. 2012); *see also United States v. Omar*, 786 F.3d 1104, 1110 (8th Cir. 2015) (citing *United States v. Isa*, 923 F.2d 1300, 1306 (8th Cir. 1991)); *United States v. Sarkissian*, 841 F.2d 959, 964 (9th Cir. 1988) (quoting *Belfield*, 692 F.2d at 147); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (quoting *Belfield*, 692 F.2d at 147).[14] In fact, every court but one (whose decision was subsequently overturned by an appellate court)[15] that has addressed a motion

[14] In *Duggan*, the Second Circuit explained that disclosure might be necessary if the judge's initial review revealed potential irregularities such as "possible misrepresentations of fact, vague identification of persons to be surveilled or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order." 743 F.2d at 78 (quoting S. Rep. 95-604, at 58 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3960).

[15] In *United States v. Daoud*, the district court ruled that it was capable of making the determination, but nevertheless ordered the disclosure of FISA materials to the defense. No. 12 Cr 723, 2014 WL 321384, at *8 (N.D. Ill. Jan. 29, 2014). The government appealed the *Daoud* court's order to the U.S. Court of Appeals for the Seventh Circuit, which overturned the district court's decision to disclose FISA materials, stating, "So clear is it that the materials were

to disclose FISA materials or to suppress FISA information has been able to reach a conclusion as to the legality of the FISA collection at issue based on its *in camera, ex parte* review. *See, e.g.*, *El-Mezain*, 664 F.3d at 566 (quoting district court's statement that no court has ever held an adversarial hearing to assist the court); *United States v. Stewart*, 590 F.3d 93, 126-28 (2d Cir. 2009); *In re Grand Jury Proceedings of the Special Apr. 2002 Grand Jury (In re Grand Jury Proceedings)*, 347 F.3d 197, 203 (7th Cir. 2003) (noting that no court at the time had ordered disclosure of FISA materials); *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987); *Mohammad*, 339 F. Supp. 3d at 737; *Abu-Jihaad*, 531 F. Supp. 2d at 310, *aff'd*, 630 F.3d at 129-30; *United States v. Rosen*, 447 F. Supp. 2d 538, 546 (E.D. Va. 2006); *United States v. Sattar*, No. 02-CR-395, 2003 WL 22137012, at *6 (S.D.N.Y. Sept. 15, 2003) (citing *United States v. Nicholson*, 955 F. Supp. 588, 592 & n.11 (E.D. Va. 1997)) (noting "this court knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance").

As the exhibits in the Sealed Appendix make clear, there is nothing extraordinary about the FISA-authorized electronic surveillance in this case that would justify the production and disclosure of highly sensitive and classified FISA

---

properly withheld from defense counsel that there is no need for a remand to enable the district judge to come to the same conclusion, because she would have to do so." *United States v. Daoud*, 755 F.3d 479, 485 (7th Cir. 2014).

materials or the suppression of FISA-obtained or -derived evidence. Here, the FISA materials are well-organized and easily reviewable by the Court *in camera* and *ex parte*, and they are fully and facially sufficient to allow the Court to make an accurate determination that the FISA information was lawfully acquired and that the electronic surveillance was made in conformity with an order of authorization or approval. In other words, the materials presented "are straightforward and readily understood." *In re Kevork*, 634 F. Supp. 1002, 1008 (C.D. Cal. 1985), *aff'd*, 788 F.2d 566 (9th Cir. 1986). Moreover, as in other cases, "[t]he determination of legality in this case is not complex." *Belfield*, 692 F.2d at 147; *see also United States v. Hasbajrami*, No. 11-CR-623 (JG), 2016 WL 1029500, at *14 (E.D.N.Y. Feb. 18, 2016) (finding the review of the FISA materials was "relatively straightforward and not complex" such that the court "was able to evaluate the legality of the challenged surveillance without concluding that due process first warranted disclosure") (internal quotations and citations omitted). This Court, much like the aforementioned courts, is capable of reviewing the FISA materials *in camera* and *ex parte* and making the requisite legal determination without an adversarial hearing.

In addition to the specific harm that would result from the disclosure of the FISA materials in this case, which is detailed in the classified declaration of an Assistant Director of the FBI in support of the Attorney General's Declaration and

Claim of Privilege, the underlying rationale for non-disclosure is clear: "In the sensitive area of foreign intelligence gathering, the need for extreme caution and sometimes even secrecy may not be overemphasized." *United States v. Ott*, 637 F. Supp. 62, 65 (E.D. Cal. 1986), *aff'd*, 827 F.2d 473 (9th Cir. 1987); *United States v. Medunjanin*, No. 10-CR-19-1, 2012 WL 526428, at *9 (S.D.N.Y. Feb. 16, 2012) (finding persuasive the government's argument that "unsealing the FISA materials in this case would provide the defense with unnecessary details of an extraordinarily sensitive anti-terrorism investigation"); *Amawi*, 531 F. Supp. 2d at 838 (finding that the FISA materials contained considerable "operational and technical information" the disclosure of which could adversely affect the government's ability to obtain "useful foreign intelligence information").

Confidentiality is critical to national security. "If potentially valuable intelligence sources" believe that the United States "will be unable to maintain the confidentiality of its relationship to them, many [of those sources] could well refuse to supply information. . . ." *Central Intelligence Agency v. Sims*, 471 U.S. 159, 175 (1985). When considering whether the disclosure of classified sources, methods, techniques, or information would harm the national security, federal courts have expressed a great reluctance to replace the considered judgment of Executive Branch officials charged with the responsibility of weighing a variety of subtle and complex factors in determining whether the disclosure of information

may lead to an unacceptable risk of compromising the intelligence gathering process, and determining whether foreign agents, spies, and terrorists are capable of piecing together a mosaic of information that, if revealed, could reasonably be expected to harm the national security of the United States. *See Sims*, 471 U.S. at 180; *Amawi*, 531 F. Supp. 2d at 837 (refusing to "second-guess" the Attorney General's declaration stating that disclosure or an adversary hearing would harm national security). An adversary hearing is not only unnecessary to aid the Court in the straightforward task before it, but such a hearing would also create potential dangers that courts have consistently sought to avoid. As the *Belfield* court explained:

> Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements. The statute is meant to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." In FISA the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law enforcement surveillance.

692 F.2d at 148 (footnotes and citations omitted).

2. *In Camera, Ex Parte* Review Is Constitutional

The constitutionality of FISA's *in camera, ex parte* review provisions has been affirmed by every federal court that has considered the matter, including the Sixth Circuit. *See United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005) ("FISA's requirement that the district court conduct an *ex parte, in camera* review of FISA materials does not deprive a defendant of due process"); *see also Abu-Jihaad*, 630 F.3d at 129 (affirming district court's determination that "its *in camera, ex parte* review permitted it to assess the legality of the challenged surveillance and the requirements of due process did not counsel otherwise"); *Stewart*, 590 F.3d at 126 (noting that "the procedures fashioned in FISA [are] a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information." (quoting *Duggan*, 743 F. 2d at 73)); *El-Mezain*, 664 F.3d at 567; *ACLU Found. of So. Cal. v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991) (procedure under FISA "is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance" (citing *Belfield*, 692 F.2d at 141)); *Ott*, 827 F.2d at 476-77.

In summary, FISA mandates a process by which the district court must review FISA applications, orders, and related materials to determine whether the

FISA information was lawfully acquired and whether the electronic surveillance was made in conformity with an order of authorization or approval. In this case, the Attorney General has filed the required declaration invoking that procedure and has declared that disclosure or an adversary hearing would harm national security. Accordingly, an *in camera, ex parte* review by this Court is the appropriate method to determine whether the FISA information was lawfully acquired and whether the electronic surveillance was conducted in conformity with an order of authorization or approval.

B. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

In evaluating the legality of the FISA collection, a district court's review should determine: (1) whether the certification submitted by the Executive Branch in support of a FISA application was properly made; (2) whether the application established the probable cause showing required by FISA; and (3) whether the collection was properly minimized. *See Abu-Jihaad*, 630 F.3d at 130-31; *see also* 50 U.S.C. §1806(f).

1. Standard of Review of Probable Cause

Although federal courts are not in agreement as to whether the FISC's probable cause determination should be reviewed *de novo* or accorded due deference, the material under review here satisfies either standard of review. *See Omar*, 786 F. 3d at 1112 ("[W]e have no hesitation concluding that probable cause

under FISA existed under any standard of review."); *Abu-Jihaad*, 630 F.3d at 130 ("Although the established standard of judicial review applicable to FISA warrants is deferential, the government's detailed and complete submissions in this case would easily allow it to clear a higher standard of review"). The government respectfully submits that it is appropriate to accord due deference to the findings of the FISC, but notes that a number of courts, including district courts in the Sixth Circuit, have reviewed the FISC's probable cause determination *de novo*.[16] While in the minority, other courts have afforded due deference to the findings of the FISC. *Abu-Jihaad*, 630 F.3d at 130; *accord United States v. Ahmed*, No. 1:06-CR-147, 2009 U.S. Dist. LEXIS 120007, at *21-22 (N.D. Ga. Mar. 19, 2009) (FISC's "determination of probable cause should be given 'great deference' by the reviewing court") (citing *Illinois v. Gates*, 462 U.S. at 236).

In the analogous area of criminal searches and surveillance, the law in the Sixth Circuit, as well as that in other federal circuits, accords great deference to a magistrate judge's probable cause determinations. *See, e.g.*, *United States v. Allen*, 211 F.3d 970, 973 (6th Cir. 2000); *see also United States v. Krupa*, 658 F.3d 1174,

[16] *See, e.g.*, *Mohammad*, 339 F. Supp. 3d at 736; *United States v. Alwan*, No. 1:11-CR-13, 2012 WL 399154, at *8-10 (W.D. Ky. Feb. 7, 2012); *United States v. Warsame*, 547 F. Supp. 2d 982, 990 (D. Minn. 2008) (citing *Illinois v. Gates*, 462 U.S. 213, 214 (1983)); *Rosen*, 447 F. Supp. 2d at 545; *United States v. Kashmiri*, No. 09-CR-830-4, 2010 WL 4705159, at *1 (N.D. Ill. Nov. 10, 2010). In each of these cases, the courts applied a *de novo* standard in reviewing the FISC's probable cause findings, and each court found the applications before it contained probable cause.

1177 (9th Cir. 2011); *United States v. Smith*, 581 F.3d 692, 694 (8th Cir. 2009); *United States v. Joseph*, 709 F.3d 1082, 1093 (11th Cir. 2013) (citing *Illinois v. Gates*, 462 U.S. at 236); *United States v. Robinson*, 724 F.3d 878, 884 (7th Cir. 2013). It would thus be consistent for a court that is reviewing FISA-authorized electronic surveillance to adopt the same posture it would when reviewing the probable cause determination of a criminal search warrant issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure. *See Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *21-22 (according the same deference to the FISC's probable cause determination as to a magistrate's criminal probable cause determination); *cf. United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (concluding that a FISA order can be considered a warrant since it is issued by a detached judicial officer and is based on a reasonable showing of probable cause).

2. Probable Cause Standard

FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. 50 U.S.C. §1805(a). It is this standard – not the standard applicable to criminal search warrants – that this Court must apply. *See Omar*, 786 F.3d at 1111 ("[R]ather than focusing on probable cause to believe that a person has committed a crime, the FISA standard focuses on the status of the

target as a foreign power or an agent of a foreign power.") (quoting *El-Mezain*, 664 F.3d at 564); *United States v. Duka*, 671 F.3d 329, 338 (3d Cir. 2011); *Cavanagh*, 807 F.2d at 790 (citing *United States v. United States District Court*, 407 U.S. 297, 322 (1972)); *Medunjanin*, 2012 WL 526428, at *6 ("[N]o branch of government – whether executive or judicial – need make a probable cause finding of *actual or potential* criminal activity to justify a FISA warrant."); *Alwan*, 2012 WL 399154, at *5.

[CLASSIFIED MATERIAL REDACTED]

3. Standard of Review of Certifications

Certifications submitted in support of a FISA application should be "subjected to only minimal scrutiny by the courts," and are "presumed valid." *Duggan*, 743 F.2d at 77 & n.6 (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978)); *United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008) (quoting *Badia*, 827 F.2d at 1463); *United States v. Sherifi*, 793 F. Supp. 2d 751, 760 (E.D.N.C. 2011); *Warsame*, 547 F. Supp. 2d at 990. When a FISA application is presented to the FISC, "[t]he FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Mohammad*, 339 F. Supp. 3d at 736 (quoting *Duggan*, 743 F.2d at 77). Likewise, "Congress intended that . . . a reviewing [district] court should have no greater authority to second-guess the

executive branch's certifications than has the FISA judge." *Duggan*, 743 F. 2d at 77; *see also In re Grand Jury Proceedings*, 347 F.3d at 204-05; *Badia*, 827 F.2d at 1463; *United States v. Rahman*, 861 F. Supp. 247, 250 (S.D.N.Y. 1994), *aff'd*, 189 F. 3d 88 (2d Cir. 1999); *United States v. Islamic Am. Relief Agency (IARA)*, No. 07-00087-CR-W-NKL, 2009 WL 5169536, at *4 (W.D. Mo., Dec. 21, 2009); *Kashmiri*, 2010 WL 4705159, at *1.

The district court's review should determine whether the certifications were made in accordance with FISA's requirements. *See United States v. Omar*, No. Cr. 09-242, 2012 WL 2357734, at *3 (D. Minn. June 20, 2012) ("the reviewing court must presume as valid 'the representations and certifications submitted in support of an application for FISA surveillance' … absent a showing sufficient to trigger a *Franks* hearing") (quoting *Duggan*, 743 F. 2d at 77); *see also Alwan,* 2012 WL 399154, at *7 ("'The [c]ourt is not to second-guess whether the certifications were correct, but merely to ensure they were properly made.'") (quoting *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *20). When the target is a United States person, the district court should also ensure that each certification is not "clearly erroneous." *Campa*, 529 F.3d at 994; *Duggan*, 743 F.2d at 77; *Kashmiri*, 2010 WL 4705159, at *2. A "clearly erroneous" finding is established only when "although there is evidence to support it, the reviewing court on the [basis of the] entire evidence is left with the definite and firm conviction that a mistake has been committed."

United States v. U.S. Gypsum Co., 333 U.S. 364, 395 (1948); *United States v. Garcia*, 413 F.3d 201, 222 (2d Cir. 2005); *IARA*, 2009 WL 5169536, at *4 (identifying "clearly erroneous" standard of review for FISA certifications).

4. FISA Is Subject to the "Good Faith" Exception

Even assuming *arguendo* that this Court determines that a particular FISC order was not supported by probable cause, or that one or more of the FISA certification requirements were not met, the evidence obtained or derived from the FISA-authorized electronic surveillance is, nonetheless, admissible under the "good faith" exception to the exclusionary rule articulated in *United States v. Leon*, 468 U.S. 897 (1984). *See Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *25 n.8, 26-27 (noting that federal officers are entitled to rely in good faith on a FISA warrant (citing *United States v. Ning Wen*, 477 F.3d 896, 897 (7th Cir. 2007))); *see also Duka*, 671 F.3d at 347 (finding "exclusionary rule plainly does not apply" to FISA-derived evidence "even if [the court] agreed with defendants that the 'significant purpose' test is unconstitutional").

In *Illinois v. Krull*, the Supreme Court "ruled categorically that 'suppressing evidence obtained by an officer acting in objectively reasonable reliance on a statute' would not further the purposes of the exclusionary rule, even if that statute is later declared unconstitutional." *Duka*, 671 F.3d at 346-37 (quoting *Krull*, 480 U.S. 340, 349-50 (1987)). The exclusionary rule should not be imposed to punish

an officer who acts in objectively reasonable reliance on a duly enacted statute. "Because the rule 'is designed to deter police misconduct,' it applies only where it will 'alter the behavior of individual law enforcement officers or the policies of their departments.'" *Duka*, 671 F.3d at 346 (quoting *Leon*, 468 U.S. at 916-18). Here, the exclusion of evidence would serve no such deterrent purpose. *See Davis v. United States*, 564 U.S. 229, 237 (2011); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 282-84 (S.D.N.Y. 2000).

In this case, there is no basis to find that any declarations or certifications at issue in this case were deliberately or recklessly false. *See Leon*, 468 U.S. at 914-15; *Massachusetts v. Sheppard*, 468 U.S. 981, 987-88 (1984). Further, there are no facts indicating that the FISC failed to act in a neutral and detached manner in authorizing the electronic surveillance at issue. *See Leon*, 468 U.S. at 914-15. Moreover, as the Court will see from its *in camera, ex parte* review of the FISA materials, facts establishing the requisite probable cause were submitted to the FISC, the FISC's orders contained all of the requisite findings, and "well-trained officers" reasonably relied on those orders. Therefore, in the event that the Court questions whether a particular FISC order was supported by sufficient probable cause, the information obtained pursuant to that order would be admissible under *Leon*'s good faith exception to the exclusionary rule.

IV. THE FISA INFORMATION WAS LAWFULLY ACQUIRED AND THE ELECTRONIC SURVEILLANCE WAS MADE IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

[CLASSIFIED MATERIAL REDACTED

A. THE INSTANT FISA APPLICATION(S) MET FISA'S PROBABLE CAUSE STANDARD

[CLASSIFIED MATERIAL REDACTED]

B. THE CERTIFICATION(S) COMPLIED WITH FISA

[CLASSIFIED MATERIAL REDACTED]

1. Foreign Intelligence Information

[CLASSIFIED MATERIAL REDACTED]

2. "A Significant Purpose"

[CLASSIFIED MATERIAL REDACTED]

3. Information Not Reasonably Obtainable Through Normal Investigative Techniques

[CLASSIFIED MATERIAL REDACTED]

C. THE ELECTRONIC SURVEILLANCE WAS CONDUCTED IN COMFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

[CLASSIFIED MATERIAL REDACTED]

1. The Minimization Procedures

Once a reviewing court is satisfied that the FISA information was lawfully acquired, it must then examine whether the electronic surveillance was lawfully conducted. *See* 50 U.S.C. § 1806(e)(2). To do so, the reviewing court must

determine whether the government followed the relevant minimization procedures to appropriately minimize the information acquired pursuant to FISA.

[CLASSIFIED MATERIAL REDACTED]

FISA's legislative history and the applicable case law demonstrate that the definitions of "minimization procedures" and "foreign intelligence information" were intended to take into account the realities of collecting foreign intelligence because the activities of persons engaged in clandestine intelligence gathering or international terrorism are often not obvious on their face. The degree to which information is required to be minimized varies somewhat given the specifics of a particular investigation, such that less minimization at acquisition is justified when "the investigation is focusing on what is thought to be a widespread conspiracy" and more extensive surveillance is necessary "to determine the precise scope of the enterprise." *In re Sealed Case*, 310 F.3d 717, 741 (FISA Ct. Rev. 2002). Furthermore, the activities of foreign powers and their agents are often not obvious from an initial or cursory overhear of conversations. To the contrary, agents of foreign powers frequently engage in coded communications, compartmentalized operations, the use of false identities and other practices designed to conceal the breadth and aim of their operations, organization, activities and plans. *See, e.g., United States v. Salameh*, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two conspirators involved in the 1993 bombing of the World Trade Center in New

York referred to the bomb plot as the "study" and to terrorist materials as "university papers"). As one court explained, "[i]nnocuous-sounding conversations may in fact be signals of important activity; information on its face innocent when analyzed or considered with other information may become critical." *Kevork*, 634 F. Supp. at 1017 (quoting H.R. Rep. No. 95-1283, pt. 1, at 55 (1978)). One court recognized that "the Congress that enacted FISA observed that 'bits and pieces of information, which taken separately could not possibly be considered "necessary" may together over time take on significance.'" *Medunjanin*, 2012 WL 526428, at *4 (quoting H.R. Rep. No. 95-1283, pt. 1, at 58-59). As a result, "courts have construed 'foreign intelligence information' broadly and sensibly allowed the government some latitude in its determination of what is foreign intelligence information." *Rosen*, 447 F. Supp. 2d at 551.

The nature of the foreign intelligence information sought also impacts implementation of the minimization procedures at the retention and dissemination stages. There is a legitimate need to conduct a thorough post-acquisition review of FISA information that involves a United States person who is acting as an agent of a foreign power. As Congress explained:

> It is "necessary" to identify anyone working with him in this network, feeding him information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts

> and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

H.R. Rep. No. 95-1283, pt. 1, at 58. Indeed, at least one court has cautioned that, when a United States person communicates with an agent of a foreign power, the government would be "remiss in meeting its foreign counterintelligence responsibilities" if it did not thoroughly "investigate such contacts and gather information to determine the nature of those activities." *United States v. Thomson*, 752 F. Supp. 75, 82 (W.D.N.Y. 1990).

In light of these realities, Congress recognized that "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." *See* S. Rep. No. 95-701, at 39 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4008 (quoting *United States v. Bynum,* 485 F.2d 490, 500 (2d Cir. 1973)). The Fourth Circuit reached the same conclusion in *United States v. Hammoud*, stating that the "mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance." 381 F.3d 316, 334 (4th Cir. 2004), *rev'd on other grounds*, 543 U.S. 1097 (2005), *op. reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005).

Accordingly, in reviewing the adequacy of minimization efforts, the test to be applied is neither whether innocent conversations were intercepted, nor whether mistakes were made with respect to particular communications. Rather, as the U.S. Supreme Court stated in the context of Title III surveillance, there should be an "objective assessment of the [agents'] actions in light of the facts and circumstances confronting [them] at the time." *Scott v. United States*, 436 U.S. 128, 136 (1978). "The test of compliance is 'whether a good-faith effort to minimize was made.'" *United States v. Mubayyid*, 521 F. Supp. 2d 125, 135 (D. Mass. 2007); *see also Sattar*, 2003 WL 22137012, at *10-11; S. Rep. No. 95-701, at 39-40, 1978 U.S.C.C.A.N., at 4008-09 (stating that the court's role is to determine whether "on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could do to avoid unnecessary intrusion").

Moreover, as noted above, FISA expressly states that the government is not required to minimize information that is "evidence of a crime," whether or not it is also foreign intelligence information. 50 U.S.C. §§ 1801(h)(3), 1821(4)(c); *see also Isa*, 923 F.2d at 1304 (noting that "[t]here is no requirement that the 'crime' be related to foreign intelligence"). As a result, to the extent that certain communications of a United States person may be evidence of a crime or otherwise

may establish an element of a substantive or conspiratorial offense, such communications need not be minimized. *See id.* at 1305.

Assuming, for the sake of argument, that certain communications were not minimized in accordance with the SMPs, suppression would not be the appropriate remedy with respect to those communications that met the standard. *Cf. United States v. Falcone*, 364 F. Supp. 877, 886-87 (D.N.J. 1973), *aff'd*, 500 F.2d 1401 (3d Cir. 1974) (Title III). As discussed above, absent evidence that "on the whole" there has been a "complete" disregard for the minimization procedures, the fact that some communications should have been minimized does not affect the admissibility of others that were properly acquired and retained. FISA's legislative history reflects that Congress intended only a limited sanction for errors of minimization:

> As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

H.R. Rep. No. 1283, pt. 1, at 93; *see also Falcone*, 364 F. Supp. at 886-87; *Medunjanin*, 2012 WL 526428, at *12 (disclosure and suppression not warranted where "failure to adhere to [the minimization] protocol was *de minimis*").

2. The FISA Information Was Appropriately Minimized

[CLASSIFIED MATERIAL REDACTED]

Based upon this information, we respectfully submit that the government lawfully conducted the FISA collection discussed herein. Consequently, for the reasons stated above, the Court should find that the FISA collection discussed herein was lawfully conducted under the minimization procedures approved by the FISC and applicable to the FISA collection discussed herein.

V. THE COURT SHOULD REJECT THE DEFENDANT'S LEGAL ARGUMENTS

The defendant seeks: (1) a determination by the government regarding the submission of an affidavit from the Attorney General attesting that disclosure of "the FISA application, FISA Order, and all cogent materials thereto" (*i.e.*, the FISA materials) would harm the national security; (2) a copy of any such affidavit; (3) an *in camera, ex parte* review of the FISA materials by this Court to determine whether the surveillance was lawfully authorized and appropriately conducted; and (4) disclosure of the FISA materials. (Doc. 28 at 22-23). As explained above, pursuant to FISA, the government is filing herewith an affidavit in which the Attorney General claims under oath that disclosure of the FISA materials or an adversary hearing would harm the national security of the United States. *See* 50 U.S.C. § 1806(f). That affidavit is included in the public, unclassified filing; thus, the defendant will have access to it. As the defendant's motion correctly stated,

the statute requires that this Court "shall" review the FISA materials *in camera* and *ex parte* to determine whether the surveillance at issue was lawfully authorized and conducted. (Doc. 28 at 3-4). *See* 50 U.S.C. § 1806(f). As the Court will see through *ex parte*, *in camera* review of the FISA materials, disclosure of the FISA materials is not necessary to make an accurate determination of the legality of the surveillance at issue. Accordingly, the defendant's demand for disclosure of the FISA materials must be denied.[17]

A. THE GOVERNMENT HAS COMPLIED WITH FISA'S MINIMIZATION REQUIREMENTS

The defendant claims that, "[t]his court is empowered to disclose FISA related materials to defendant because 'such disclosure is necessary to make an accurate determination of the legality of the surveillance.'" (Doc. 28 at 6) (quoting 50 U.S.C. § 1806(f)). The defendant omitted two key words when quoting FISA: "only where." This Court may disclose the FISA materials "*only where* such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. §1806(f) (emphasis added). The Court must conduct its review of those materials *in camera* and *ex parte*, and disclosure is within the Court's discretion only following that review and only if the Court is unable to

[17] To the extent that this Court construes any of the defendant's arguments as supporting suppression of the FISA materials, the government respectfully submits that, for the reasons discussed herein, the surveillance was lawfully authorized and conducted; therefore, there is no basis for suppression.

determine the legality of the electronic surveillance without the assistance of defense counsel. *See Amawi,* 531 F. Supp. 2d at 837 ("Where on the basis of what it receives from the government *in camera* and under seal, a district court concludes that it can determine whether a FISA surveillance and search was lawful, it may not order disclosure of any of the FISA materials."). If the district court is able to make an accurate determination of the legality of the electronic surveillance based on its *in camera, ex parte* review of the materials submitted by the United States, then the court *may not* order disclosure of any of the FISA materials to the defense, unless otherwise required by due process. *See Abu-Jihaad,* 630 F.3d at 129 (quoting 50 U.S.C. § 1806(g)); *El-Mezain*, 664 F.3d at 566; *Mohammad*, 339 F. Supp. 3d at 737.

This holding is fully supported by the legislative history of 50 U.S.C. § 1806(f), which states: "The court may order disclosure to [the defense] only if it finds that such disclosure is necessary to make an accurate determination of the legality of the surveillance . . . . Once a judicial determination is made that the surveillance was lawful, a motion for discovery . . . must be denied." S. Rep. No. 95-701, at 64-65. As this Court will see from its review, the FISA materials are presented in a well-organized and straightforward manner that will allow the Court to make its determination of the lawfulness of the FISA collection without input from defense counsel.

In support of the claim that disclosure "is necessary and proper to make an accurate determination of the legality of the surveillance," the defendant cites to FISA's legislative history and case law stating,

> in determining whether disclosure is necessary, the court should consider whether after its initial review, and [sic] irregularities are revealed, such as whether the materials evidence a possible misrepresentation of fact; the persons to be surveilled are not clearly identified; or the surveillance records include a significant amount of non-foreign intelligence information, indicating a possible issue with the minimization standard utilized.

(Doc. 28 at 6-7) (quoting *United States v. Mahamud*, 838 F. Supp. 2d 881, 885 (D. Minn. 2012)). The defendant does not allege misrepresentations of fact or the failure to identify the persons to be surveilled. However, the defendant claims that in this case "the surveillance was for domestic intelligence information, or alternatively was a significant amount of non-foreign intelligence information, both in violation of the minimization procedure." (Doc. 28 at 7). The defendant points to the requirement that a FISA application establish probable cause that the target is a foreign power or an agent of a foreign power, though he does not specifically allege that the government did not satisfy the probable cause requirements of FISA. (Doc. 28 at 8). The defendant also claims that he was charged with a crime that "ha[s] absolutely nothing to do with national security." (Doc. 28 at 10).

[CLASSIFIED MATERIAL REDACTED]

The defendant's argument that the acquisition of a significant amount of non-foreign intelligence information violates the minimization procedures similarly fails. FISA was drafted with the intent to provide "latitude" to the government with regard to minimization. *Rosen*, 447 F. Supp. 2d at 552 (citing House Report, part 1, at 58). In addressing minimization, "courts have construed 'foreign intelligence information' broadly and sensibly allowed the government some latitude in its determination of what is foreign intelligence information." *Rosen*, 447 F. Supp. 2d at 551. Guided by these principles, courts have rejected the defendant's argument. *See id.* at 546 (defendants' "claim that the discovery obtained from the government contains a significant amount of non-foreign intelligence information . . . relies upon an inordinately narrow view of what constitutes foreign intelligence information, and is therefore unavailing").

[CLASSIFIED MATERIAL REDACTED]

B. THE GOVERNMENT HAS COMPLIED WITH THE FOURTH AMENDMENT

The defendant calls into question the purpose of the electronic surveillance at issue, alleging, "the government obtained a FISA order against defendant even though their primary purpose was for a domestic criminal prosecution, and their action(s) violated the Fourth Amendment." (Doc. 28 at 13). First, the defendant claims that because the defendant has not committed any of the delineated

"international criminal acts, . . . [t]he government's case must be dismissed with prejudice for violation of § 1806(k)." *Id.* The defendant misconstrues 50 U.S.C. § 1806(k), which allows federal officers who conduct electronic surveillance to acquire foreign intelligence information to consult with federal law enforcement officers to coordinate efforts to investigate or protect against actual or potential attack or other grave hostile acts, sabotage, or international terrorism, or clandestine intelligence activities, by foreign powers or their agents. The purpose of this provision, which was added with the passage of the USA PATRIOT Act in 2001, was to "expressly sanction[] consultation and coordination between intelligence and law enforcement officials . . . ." *In re Sealed Case*, 310 F. 3d at 728-29. "[S]uch coordination 'shall not preclude' the government's certification that a significant purpose of the surveillance is to obtain foreign intelligence information, or the issuance of an order authorizing surveillance." *Id.* at 729 (quoting 50 U.S.C. § 1806(k)(1)). That provision cannot properly be read, as defendant seemingly does, to prohibit consultation and coordination to investigate or protect against crimes that do not have an obvious nexus to national security. To the contrary, the statute permits the government to retain and disseminate evidence of other crimes.

As part of the USA PATRIOT Act, Congress also "amended FISA to change 'the purpose' language of 1804(a)(7)(B) to 'a significant purpose.'" *Id.* The

defendant appears to concede that the "significant purpose" requirement is constitutional when he states, "electronic surveillance may proceed without the protections of a traditional warrant based on probable cause only if a court determines that the 'significant purpose' of the surveillance is to obtain foreign intelligence information." (Doc. 28 at 21).[18] The "significant purpose" test has been repeatedly upheld, including recently by another district court in the Sixth Circuit. In *Mohammad*, the court rejected the defendants' claim that decisions upholding the constitutionality of the "significant purpose" test should be revisited in light of public disclosures regarding government surveillance programs. The court ruled that the Sixth Circuit's decision in *Damrah* continued to be controlling precedent and foreclosed the defendants' Fourth Amendment challenge. 339 F. Supp. 3d at 739 (citing *Damrah*, 412 F. 3d at 625). Indeed, every court that has addressed this issue has found the significant purpose test to be reasonable under the Fourth Amendment. *See, e.g., Duka*, 671 F3d. at 343 ("We agree with our sister courts of appeals and the Foreign Intelligence Surveillance Court of Review that the amended FISA's 'significant purpose' standard is reasonable under the Fourth Amendment."); *Abu-Jihaad,* 630 F.3d at 128 ("We conclude simply that FISA's 'significant purpose' requirement . . . is sufficient to ensure that the

[18] The defendant cites to *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991) to support that proposition. However, *Johnson* was decided prior to passage of the Patriot Act in 2001, and therefore, prior to the inclusion of the "significant purpose" language.

executive may only use FISA to obtain a warrant when it is in good faith pursuing foreign intelligence gathering . . . ."); *Ning Wen*, 477 F.3d at 897; *Damrah*, 412 F.3d at 625; *In re Sealed Case,* 310 F.3d at 746; *Mubayyid,* 521 F. Supp. 2d at 139; *United States v. Marzook*, 435 F. Supp. 2d 778, 786 (N.D. Ill. 2006); *United States v. Benkahla*, 437 F. Supp. 2d 541, 554 (E.D. Va. 2006).

The defendant even appears to concede that the government satisfied the "significant purpose" standard in this case.[19] The defense motion states, "In the case at bar the purpose of the FISA Order was to secure foreign intelligence for National Security. However, the government's evidence gathering against defendant was *per-se* for domestic criminal prosecution." (Doc. 28 at 21-22). Such an argument ignores that the government, in conducting lawful foreign intelligence surveillance, may properly retain and disseminate evidence of crimes. *See* 50 U.S.C. §1801(h)(3) (requiring that court-approved foreign intelligence minimization procedures "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes"); *Ning Wen*, 477 F.3d at 898 ("If, while conducting [FISA] surveillance, agents discover evidence of a domestic crime, they may use it to prosecute for that offense."); *Duggan*, 743 F.2d at 78 ("[W]e emphasize that otherwise valid FISA surveillance

[19] **[CLASSIFIED MATERIAL REDACTED]**

is not tainted simply because the government can anticipate that the fruits of such surveillance may later be used, as allowed by [50 U.S.C.] § 1806(b), as evidence in a criminal trial."); *see In re Sealed Case*, 310 F.3d at 731 ("minimization procedures allow . . . the retention and dissemination of non-foreign intelligence information which is evidence of *ordinary crimes* for preventative or prosecutorial purposes.").

Moreover, the fact that criminal prosecution is one of the possible purposes is not fatal.[20] *See Abu-Jihaad*, 630 F.3d at 128-29; *In re Sealed Case,* 310 F.3d at 735. The fact that "the government may later choose to prosecute is irrelevant," as "FISA contemplates prosecution based on evidence gathered through surveillance" to secure foreign intelligence information. *Sarkissian*, 841 F.2d at 965. The *Abu-Jihaad* court rejected the argument that FISA is unconstitutional because it does not require certification of a primary purpose to obtain foreign intelligence information and stated, "The fact that the government may also be pursuing other purposes, including gathering evidence for criminal prosecution, compels no different conclusion." *Id.* at 128-29. Accordingly, the defendant's claim that the government violated the Fourth Amendment is without merit. For these reasons, the Court should deny the defendant's request for disclosure of the FISA materials.

---

[20] A criminal prosecution motive is only fatal if the Court finds the Government's significant purpose certification in the FISA application is clearly erroneous. *See Abu-Jihaad,* 630 F.3d at 128.

VI. CONCLUSION: THERE IS NO BASIS FOR THE COURT TO SUPPRESS THE FISA INFORMATION OR DISCLOSE THE FISA MATERIALS

Based on the foregoing analysis, the government respectfully submits that the Court must conduct an *in camera*, *ex parte* review of the FISA materials and the government's classified submission, and should: (1) find that the electronic surveillance at issue in this case was both lawfully authorized and lawfully conducted in compliance with FISA; (2) hold that disclosure of the FISA materials and the government's classified submissions to the defendant is not authorized because the Court is able to make an accurate determination of the legality of the surveillance without disclosing the FISA materials or any portions thereof; (3) hold that the fruits of the electronic surveillance should not be suppressed; (4) deny the defendant's motion without an evidentiary hearing; and (5) order that the FISA materials and the government's classified submissions be maintained under seal by the Classified Information Security Officer or his or her designee.[21]

[21] A district court order granting motions or requests under 50 U.S.C. § 1806(g), a decision that electronic surveillance was not lawfully authorized or conducted, and an order requiring the disclosure of FISA materials is each a final order for purposes of appeal. 50 U.S.C. § 1806(h). Should the Court conclude that disclosure of any item within any of the FISA materials or suppression of any FISA-obtained or -derived information may be required, given the significant national security consequences that would result from such disclosure or suppression, the government would expect to pursue an appeal. Accordingly, the government respectfully requests that the Court stay any such order pending an appeal by the United States of that order.

Respectfully submitted,

MATTHEW SCHNEIDER
United States Attorney

/s/ Cathleen M. Corken
Cathleen M. Corken
Craig Weier
Assistant United States Attorneys
211 W. Fort Street, Suite 2001
Detroit, MI 48226
Phone (313) 226-9100

Attorneys for United States of America